NIST SP 800-63, *Electronic Authentication Guideline* and Biometrics

Mar. 30, 2005

Bill Burr
william.burr@nist.gov

Authentication Policy and Guidance

- **OMB M0404 Policy Guidance for e-authentication**
  - Agencies classify electronic transactions into 4 levels needed authentication assurance according to the potential consequences of an authentication error
    - Consider: privacy, inconvenience, damage to reputation, harm to agencies and programs, financial liability, crime, safety
- **NIST SP 800-63: Technical authentication Framework for remote e-authentication**
  - http://csrc.nist.gov/publications/nistpubs/index.html
  - Establishes technical requirements for 4 levels of M0404 for
    - Identity proofing requirements
    - Authentication protocols and mechanisms based on secrets
- **Homeland Security Presidential Directive 12**
  - FIPS 201 will deal with local and remote authentication credentials for Federal employees and contractors
  - Short schedule: 6 months for NIST from August 2004

Max. Potential Impacts Profiles

Potential Impact Categories for Authentication Errors	*Assurance Level Impact Profiles*			
	1	2	3	4
Inconvenience, distress, reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency prog. or pub. interests	N/A	Low	Mod	High
Unauth. release of sensitive info	N/A	Low	Mod	High
Personal safety	N/A	N/A	Low	Mod High
Civil or criminal violations	N/A	Low	Mod	High

Authentication: Local vs Remote

- **Local authentication**
  - —Verifier control and supervision is comparatively easy
    - Verifier controls entire authentication system
    - Claimant may be supervised (to various degrees) or unsupervised
    - Verifier knows just where claimant physically is
- **Remote authentication**
  - —Verifier control and supervision is harder
    - Claimant generally uses his own system, controls his own software
    - Claimant is generally unsupervised
    - Network access: verifier knows only that claimant has network access
    - Hardware tokens improve supervision and extend verifier control
- **NIST SP 800-63 applies to remote authentication methods using secrets**
- **FIPS 201applies to Federal Personal Identity Verification card for both physical and logical access**

Authentication Factors

- **Something you know**
  - Typically some kind of password
- **Something you have**
  - For local authentication typically an ID card
  - For remote authentication typically a cryptographic key
    - “hard” & “soft” tokens
- **Something you are**
  - A biometric
    - Unattended capture is problematic Capture can deter fraud even if not checked in authentication process
- **The more factors, the stronger the authentication**

Remote Authentication Protocols

- **Conventional, secure, remote authentication protocols all depend on proving possession of some secret "token"**
  - May result in a shared cryptographic session key, even if token is a password
- **Remote authentication protocols assume that you can keep a secret**
  - Private key, Symmetric key or Password
- **Can be "secure" against defined attacks if you keep the secret**
  - Work required for attack can be calculated or estimated
    - Make the amount of work impractical
  - People can't remember passwords strong enough to make "offline attacks" impractical
  - Good password remote authentication blocks eavesdropper attacks
    - Harder to prevent shoulder surfing or phishing

Attacks

- **Eavesdropper** – listens in
- **Decoy sites, access points and terminals,**
  - Impersonate a real site and either facilitate a man-in-the-middle attack or capture password tokens
  - Facilitated by browser limitations and ability of websites to control the user's screen appearance
  - Phishing brings victim to the decoy
- **Man-in-the-middle** - communications go through the attacker
  - Can yield attacker some tokens, allow attacker to eavesdrop, or can allow session hijacking
- **Social Engineering** – attacker persuades user to do something insecure
  - Probably no remote authentication method is entirely immune to this
- **Malware & intrusion** – bad software introduced on claimant' computer
  - Copied token: some tokens are easy to copy and the user will never know

Four technology levels of 800-63

- **Level 1 (little confidence in asserted identity)**
  - No identity proofing
  - Relatively weak passwords allowed; may be vulnerable to eavesdroppers
- **Level 2 (some confidence in asserted identity)**
  - Better passwords, but
    - Single factor & still vulnerable to phishing, social engineering, etc.
- **Level 3 (high confidence in asserted identity)**
  - Two factors, eg. password + soft crypto token or one-time password device
    - Phishing attacks shouldn't get master auth. secret
- **Level 4 (very high confidence in asserted identity)**
  - In person ID proofing
  - Hard crypto tokens required – something you tangibly have
  - Crypto binding of authentication and data transfer

Soft Tokens

- Key, typically encrypted using a key derived from a password
  - 2 factors, more or less
  - Symmetric or asymmetric key
- Protects against many attacks
  - eavesdroppers
  - Man-in-the-middle
- Key itself is vulnerable to malware and intrusion attacks
  - Very easy to copy encrypted key, and an off-line password dictionary attack on the token will very often succeed

One-time Password Devices

- **FIPS 140-1 crypto module**
  - Minimum FIPS 140 level 1
- **For 800-63 level 3 must involve a user memorized password**
- **Symmetric key devices**
- **Generate “One time Passwords” from nonce and symmetric key**
  - Password is manually entered into server like any other password
  - Works with any ordinary browser – both a virtue and a fault
- **Vulnerable to MITM attacks**
  - Largely because of browser limitations
  - But never loose the key in an MITM attack
- **Physical device, something you really have and know you have**
  - Very hard to copy

Hard Tokens

- For 800-63 a FIPS 140 validated hardware crypto token
  - FIPS 140 Level 2 with level 3 physical security needed for SP 800-63 level 4
    - Requires PIN or biometrics authentication to activate the token
- All the desirable security properties of Soft Tokens plus
  - Physical device, something you really have and know you have
    - Very hard to copy
  - Better resistance to malware and intrusion attacks
    - Not invulnerable, but the attacker won't learn the key

FIPS 201 PIV Card

Graduated Assurance Levels for Identity Authentication

PIV Assurance Level Required by Application/Resource (M-0404 level)	Applicable PIV Authentication Mechanism		
	Physical Access	**Logical Access** Local Workstation Environment	**Logical Access** Remote/Network System Environment
SOME confidence (lvl 2)	VIS, CHUID	CHUID	PKI
HIGH confidence (lvl 3)	BIO	BIO	PKI
VERY HIGH confidence (lvl 4)	BIO-A, PKI	BIO-A, PKI	PKI

Multifactor Remote Authentication

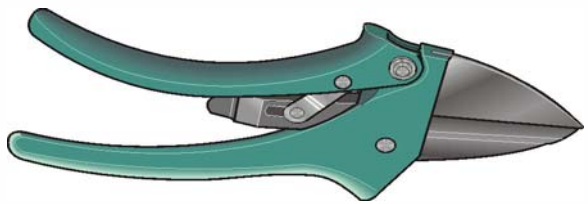
- **The more factors, the stronger the authentication**
  - Two factors required for Level 3 by 800-63
- **Multifactor remote authentication typically uses a crypto key**
  - Key is protected by a password or a biometric
  - To activate the key or complete the authentication, you need to know the password, or possess the biometric
  - Works best when the key is held in a hardware device (a “hard token”)
    - Ideally a biometric reader is built into the token, or a password is entered directly into token
- **Are there other ways?**
  - Not yet in 800-63

New ways to get to level 3?

- **Many possibilities; candidates for level 3:**
  - "Bingo Cards"
    - Human readable card with cells identified by a row and a column
    - Cell contents randomly generated
    - Challenge is the row and column
    - Reply is cell contents
  - Cell phones as tokens
    - Enter one time authenticator sent to cell with an SMS message
    - Cell phone authentication itself isn't quite FIPS strength crypto
  - Use "fingerprint" of personal computer
    - Involve Java script and cookies
    - Also use personal image to authenticate website to user
  - Biometrics too??
- **Any of these easily combined with password for second** factor
- **Can have pretty good entropy**

Biometrics

- **Biometrics tie an identity to a human body**
- **Biometric authentication depends on being having a fresh, true biometric capture, not on keeping the biometric secret**
  - Easy when the person is standing in front of you at the capture device
  - Harder if all you have is bits from anywhere on the internet
- **Biometrics aren't suitable secrets for remote authentication**
  - Hard to keep them secrets
  - Limited number per person and you can't change them
    - A feature, not a bug, it's why biometrics are so useful
    - Maybe you could revoke them, but would you like the process?



Culture Clash

- **Current remote authentication methods are mainly cryptographic**
- **Cryptographers are adversarial**
  - Propose a new crypto method and everybody tries to break it
  - Kerchoffs assumption: an adversary will know all the details of the design of your system (only secrets are operational keys)
- **Cryptographers will develop an attack and publish it in enough detail so that others can replicate their work, and think they have done good**
  - 5 hash algorithms including MD5 publicly broken at crypto 2004
  - Fluhrer/Shamir RC4 papers lead to WEPCrack & AirSnort “kiddie scripts”
  - We do this to crypto & we’ll do it to biometrics authentication too
    - Cryptographers believe that a dental technician has the skills and materials to construct a copy of a fingerprint that will fool most fingerprint readers
- **Can biometrics stand up to this kind of public, sustained attack?**
  - If they can, what about personal privacy – how much do we impact it?”

Some Workshop Issues

- We have the model of building a biometric reader into a personal cryptographic token to unlock the user's key in 800-63 now
  - How else can we get strong remote authentication with biometrics?
- What are acceptable false acceptance rates and how can we measure them?
- Can we get Level 2 with only a biometric factor?
  - Can we get to 2^{-14} false acceptance rates?
- Can we combine a password and a biometric to get to Level 3?
- For crypto tokens we have FIPS 140 validation testing: how do we get the biometric equivalent?
- How can a remote verifier know it has a fresh "real" biometric?
  - Not an old copy of a biometric and not something synthesized
- What are the privacy implications of large biometric databases?
- What is the process for working on this?

Questions

National Institute of Standards and Technology